

REMARKS

Claims 1-41 are pending in this application.

Applicant respectfully traverses the rejection of claims 1-5, 14-16, 18, 20-25, 29-34, and 38-41 under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 5,784,464 to Akiyama et al. ("*Akiyama et al.*") in view of U.S. Patent No. 5,319,705 to Halter et al. ("*Halter et al.*").

Independent claims 1 and 20 are allowable over *Akiyama et al.* and *Halter et al.* because *Akiyama et al.* and *Halter et al.* fail to teach or suggest, either alone or in combination, all of limitations of claims 1 and 20, and it would not have been obvious to one of ordinary skill to combine *Akiyama et al.* and *Halter et al.* to obtain the method recited in claim 1 or the system recited in claim 20. For example, *Akiyama et al.* and *Halter et al.* fail to teach or suggest, alone or in combination, a content management method comprising, inter alia, or a content management system comprising, inter alia, a sending means for "sending the encrypted content key and the second storage key to a key management unit," as recited in claims 1 and 20, respectively, (emphasis added).

Akiyama et al. discloses "a client authenticating system in a data distributing system having a data supplying apparatus for holding data and a client receiving the data via a communication interface from the data supplying apparatus" (col. 2, lines 46-49). "The data supplying apparatus may be [] constructed to distribute [] encrypted data to the client. In this case, the client is constructed to include a first decrypting element for decrypting the encrypted data. The data supplying apparatus may be constructed to include a third encrypting element for encrypting [a] third key for decrypting the data by use of [a] first key. In this case, the client is constructed to include a second decrypting element for decrypting the encrypted third key by use of [a] second key. Then, the first

decrypting element decrypts the encrypted data with the third key decrypted by the second decrypting element” (col. 3, lines 16-28).

The Examiner appears to rely on the “second key” of *Akiyama et al.* as allegedly constituting the “second storage key” recited in claims 1 and 20. However, *Akiyama et al.* is silent on the matter of “sending” the second key “to a key management unit,” as required by claims 1 and 20 (emphasis added). In addition, the Examiner acknowledges that *Akiyama et al.* fails to teach the “encrypted content key” recited in claims 1 and 20 (emphasis added), and relies on *Halter et al.* to allegedly make up for this deficiency (Office Action, paragraph bridging pages 7 and 8).

Halter et al. discloses “a cryptographic means for protecting software distributed over an open channel or via a high-density stamped medium” (col. 5, lines 28-30). “When a customer purchases multimedia software from a software distribution facility, the customer provides his/her customer number. The customer key is produced from a set of variables consisting of an assigned customer number, a counter (arbitrarily set to zero), and a secret key-generating key (KGK) known only to the software distribution center. A special copy-right protected function (f) is then used to derive a variant customer key (KC’) from the customer key. The data key(s) associated with the multimedia file(s) purchased by the customer are then encrypted with the variant customer key. The clear customer key and the encrypted file key(s) are provided to the customer . . . At the user processor, the keys and encrypted file(s) are initialized and made available to the file recovery program. The file recovery program decrypts and recovers the file(s).” (Col. 5, line 65 to col. 6, line 16.)

Halter et al. does not make up for the deficiencies of *Akiyama et al.* because *Halter et al.* is silent on the matter of “sending” the “second key” of *Akiyama et al.* “to a key management unit,” as required by claims 1 and 20 (emphasis added). Thus, *Halter et al.* also fails to teach or suggest “sending the encrypted content key and the second storage key to a key management unit,” as recited in claims 1 and 20.

It also would not have been obvious to one of ordinary skill to combine *Akiyama et al.* and *Halter et al.* to derive “sending the encrypted content key and the second storage key to a key management unit,” as suggested by the Examiner, because such a combination would result in an inoperable method or apparatus. There is no suggestion to modify a prior art device where the modification would render the device inoperable for its intended purpose. *In re Gordon*, 733 F.2d 900, 902, 221 USPQ 1125, 1127 (Fed. Cir. 1984); *In re Sponnoble*, 405 F.2d 578, 587, 160 USPQ 237, 244 (CCPA 1969).

The Examiner argues, “it would have been obvious . . . to modify the invention of *Akiyama et al.* by using the key distribution system disclosed by Halter, in order to prevent files from being decrypted except at appropriate user processors” (Office Action, page 3, paragraph 3). However, one of ordinary skill would understand that sending the “second key” of *Akiyama et al.* from the “client” to the “data supplying apparatus” of *Akiyama et al.* as plaintext would expose the “second key” to interception by a third party. By intercepting the “second key,” the security intended by the system of *Akiyama et al.* would be compromised. Thus, since the system of *Akiyama et al.*, as modified by the Examiner, would be inoperable for its intended purpose, it would not have been obvious for one of ordinary skill to combine *Akiyama et al.* and *Halter et al.* as suggested by the Examiner.

Moreover, even assuming *arguendo* that a “content key,” “first storage key,” “second storage key,” and “content data” can be found in *Akiyama et al.* and *Halter et al.*, which Applicant does not concede, *Akiyama et al.* and *Halter et al.* nevertheless fail to teach or suggest, either alone or in combination, “decrypting the encrypted content key using the first storage key” and “encrypting the decrypted content key using the second storage key,” as recited in claims 1 and 20 (emphasis added).

The Examiner provides a vague indication of where the “content key,” “first storage key,” and “second storage key” allegedly read on isolated elements of *Akiyama et al.* and *Halter et al.* (Office Action, page 8; paragraph 2 to page 9, paragraph 3). However, claims 1 and 20 recite the content key, first storage key, and second storage key, not in isolation, but rather within limitations such as “decrypting the encrypted content key using the first storage key” and “encrypting the decrypted content key using the second storage key” (emphasis added). The Examiner’s rejection fails to point out where all the claim limitations can allegedly be found in *Akiyama et al.* or *Halter et al.* Indeed, *Akiyama et al.* and *Halter et al.* are silent on the matter of “decrypting the encrypted content key using the first storage key” and “encrypting the decrypted content key using the second storage key,” as recited in claims 1 and 20 (emphasis added).

Thus, since *Akiyama et al.* and *Halter et al.* fail to teach or suggest, alone or in combination, each and every element of independent claims 1 and 20, and since it would not have been obvious to one of ordinary skill to combine *Akiyama et al.* and *Halter et al.* to obtain the method recited in claim 1 or the system recited in claim 20, claims 1 and 20, and claims 2-19 and 21-41, which depend therefrom, respectively, are allowable over *Akiyama et al.* and *Halter et al.*

In view of the foregoing remarks, Applicant respectfully requests reconsideration of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: July 31, 2007

By: 

Reece Nienstadt
Reg. No. 52,072